Appendix 3: Telecommunications Sector

Sector Description

The telecommunications sector provides voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks. The PSTN provides switched circuits for telephone, data, and leased point-to-point services. It consists of physical facilities, including switches, access tandems, and other equipment. These components are connected by fiber and copper cable (physical), dedicated staff to ensuring service (people), and IT systems that monitor and move the data (cyber). The physical PSTN remains the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wireless network for mobile users. The Internet is a Key Resource in which the Telecommunications Sector and the IT Sector have a shared responsibility. The Internet consists of a global network of packet-switched networks that use a common set of protocols. Internet Service Providers provide a basic service to end-users allowing them access to the Internet. Enterprise networks are dedicated networks supporting the voice and data needs and operations of large enterprises. These networks comprise a combination of leased lines or services from the PSTN or Internet providers. A few examples of sector members include wireless, landline/wireline, satellite, broadband, radio, television, HAM radio, and cable providers.

Results of Infrastructure Interruptions

Many of the interruptions that would be experienced due to a telecommunications failure are similar to those that would be seen in information technology failures.

- Telephone/Cellular/Paging Service failures.
- Data circuit, networking, private branch exchange, voicemail trunking, etc. interruptions.
- 911 Dispatch would be inoperable.
- Many government functions would halt.
- Citizens of Region 6 will not be able to contact government agencies or each other.

Regional Service Providers Active in CIP

- Cingular Wireless
- City of Bellevue
- City of Kent
- City of Redmond
- City of Renton
- City of Seattle
- King County
- Qwest Communications
- Westin Building

Current Information Sharing Mechanisms

- National Coordinating Center for Telecommunications (NCC) (http://www.ncs.gov/ncc)
- Information Technology - Information Sharing and Analysis Center (IT-ISAC), (http://www.it-isac.org)
- Coordination Center (CERT/CC) is a center of Internet security expertise, (http://www.cert.org)
- United States Computer Emergency Readiness Team (US-CERT), (http://www.us-cert.gov)
- Network Security Information Exchange (NSIE), (http://www.nsie.org)
- National Security Telecommunications Advisory Committee (NSTAC), (http://www.ncs.gov/nstac/nstac)
- Network Reliability and Interoperability Council (NRIC), (http://www.nric.org)
- National Cable & Telecommunications Association (NCTA), (http://www.ncta.com)
- Telecommunications Industry Association (TIA), (http://www.tiaonline.org/)
- Pacific Northwest Economic Region (PNWER), (http://www.pnwer.org)
- NWWARN, (https://www.nwwarn.gov)

Common Vulnerability Assessment Tools

- American National Standards Institute (ANSI) Assessment Standards
- Disaster Recovery Institute (DRI) International Vulnerability Assessment Guidelines
- Business Continuity Institute (BCI) Guidelines
- International Standards Organization (ISO) 17799 and its predecessor British Standard 7700. British Standard 7799 became ISO/IEC 17799 on November 30, 2000.
- CARVER + Shock VAM, The CARVER + Shock methodology. CARVER was originally developed by the US Special Forces.
- HLS-CAM, HLS-CAM Criticality developed by the West Virginia National Guard based on the DTRA JSIVA model modified to the civilian sector along with the Florida Domestic Security Task Force Comprehensive Vulnerability Assessment.
- IAPVA, IAP VA methodology developed by the Joint Program Office – Special Technology Countermeasures.
- State Vulnerability Assessment Methodology, The State Vulnerability Assessment (VA) Methodology developed by Argonne National Laboratory for the Department of Homeland Security (DHS) (2003).
- SVA-Pro, developed by Dyadem International Ltd. (2003).
- Terrorism VSAT, Developed by the North Carolina Department of Agriculture and Consumer Services for the North Carolina agri-business community.
- VAF, prepared under contract for the Critical Infrastructure Assurance Office by KPMG Peat Marwick LLP (1998).